CIO SECURITY COUNCIL COMMITTEE MEETING MINUTES

Wednesday, November 18, 2009
Jessie Parker Building, Knudsen Training Room

Present: Luke Bailiff, Deb Castillo, Mike Chesmore, Ruth Coleman, Deb Covington, Jean Foshier, Jeff Franklin, Kevin Eppens, Kevin Kammermeier, Shane Ludwig, Steve Mickelson, Scott Miller, Calvin Moore, Alison Radl, Steve Nicoll, John Wolf

The working groups met. Discussions are summarized below.

Emerging Threats

- Recommendations were made to add additional information to the Social Networking Best practices
- Agency reputation
- Information leakage –no redaction
- Controls or recommendations to reduce risks
- Productivity – (the cost of lost productivity)
- Introduction of malicious code
- Recommend a policy for reserving agency placeholders on social networking sites such as Facebook and Twitter so they are not exploited by outside entities (I don't recall if this was discussed in our large-group gathering)

Information Sharing

- What tools does each agency have?
- Who are the subject matter experts (SMEs) in each agency?
- Can we establish a forum or identify who the SMEs are in each agency so we can bounce ideas off one another or seek out other SMEs when we have an issue
- Meaningful quantitative data

- Use meaningful quantitative data to identify such things as network threats, e-mail viruses, etc. and report to agency administrators each month
- The intent is to provide consistent, meaningful data to inform agency administrators about current security threats and to show non-IT administrative staff the value in the security tools that IT uses to protect state networks

- Recommend a policy for reserving agency placeholders on social networking sites such as Facebook and Twitter so they are not exploited by outside entities

Policy, Standards and Best Practices Initiatives

- The group will identify contact people so important policies and other information is getting passed along in the agencies
- Document policy development process

Computer Security Awareness and Education Training

- Index Security awareness materials already available
- Develop a curriculum for security awareness training for all new employees
- Develop online training once the security awareness training is complete

- **Security Collaboration**
- Have not identified any deliverables yet
- Recommend utilizing Sharepoint as a one-stop process for information sharing and technical issues. Also had questions about what could potentially be considered public information under the freedom of information act (FOIA). *In response to that, Steve Nicoll will try to get an AG to come for our next meeting to discuss this topic
- The Security Collaboration Working Group will collaborate with Alison Radl on security research, reports, forums, etc. on the CIO Security Council Sharepoint site

Security Breach Update

- ISO briefed on recent security breaches
- The ISO is starting to classify the events
- There is currently no information reported on what triggers what action. Trying to identify what is important and what need to know.

Cyberstorm Update - ISO briefed

- Not certain to what extent agencies will participate
- Critical areas identified
  - Critical Infrastructures are law enforcement, electric, international partners, Canada, Australia, IT Community such as McAfee, Symantec, etc.

Chair of the CIO Council

- Chair of the CIO Council visited and thanked the groups for their effort
- Other important points she mentioned: get to know one another and who to call when in trouble; good efforts across the enterprise;
- Some asked what do they want the CIO Security Council group to come back to the CIO Council with?
    - To summarize -- it depends
    - CIO Council not necessarily a decision-making body but some things they can influence while others will be a recommendation to the TGB
    - Providing a list of options with recommendations is helpful for the council